

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

<p>JILLINE DOBRATZ, on behalf of herself and all others similarly situated,</p> <p style="text-align: center;">Plaintiff,</p> <p style="text-align: center;">v.</p> <p>THE MEDICAL COLLEGE OF WISCONSIN, INC. and PROGRESS SOFTWARE CORPORATION,</p> <p style="text-align: center;">Defendants.</p>	<p>Case No.: _____</p> <p><b>CLASS ACTION COMPLAINT</b></p> <p><b>DEMAND FOR JURY TRIAL</b></p>
---	---

Plaintiff Jilline Dobratz ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Defendant The Medical College of Wisconsin, Inc. ("MCW") and Defendant Progress Software Corporation ("PSC") (collectively, "Defendants") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

**INTRODUCTION**

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' sensitive information, including their full names ("personally identifiable information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

2. Defendant MCW is a corporation, based in Milwaukee, Wisconsin, that provides medical services to its patients.

3. Defendant PSC advertises itself as an “experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely.”<sup>1</sup>

4. Upon information and belief, former and current MCW patients are required to entrust Defendants with sensitive, non-public Private Information, without which Defendants could not perform their regular business activities, in order to obtain medical services from MCW. Defendants retain this information for at least many years and even after the patient-physician relationship has ended.

5. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. MCW utilized a software known as the MOVEit Transfer for the sending and receiving of sensitive information, and on an undisclosed date, MCW learned of a vulnerability in MOVEit Transfer software that had been actively exploited by unauthorized actors.<sup>2</sup> In response, MCW “immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third-party professionals to assist in the investigation and remediation of the vulnerability.”<sup>3</sup> As a result of the investigation, MCW concluded—on September

---

<sup>1</sup> <https://www.progress.com/company>

<sup>2</sup> The “Notice Letter”.

<sup>3</sup> *Id.*

21, 2023—that "certain files containing [Plaintiff's and Class Members'] personal information were potentially removed from our MOVEit server by an unauthorized party on May 27, 2023."<sup>4</sup>

7. According to the Notice of Security Incident letter sent by MCW, on behalf of Defendants, to Plaintiff and other victims of the Data Breach (the "Notice Letter"), the compromised Private Information included individuals' full names, health insurance applications and/or claims information, medical histories, conditions, treatments, and/or diagnoses information, medical procedures information, patients dates of service, and patients medical record numbers.<sup>5</sup>

8. Defendants failed to adequately protect Plaintiff's and Class Members Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect patients' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants' failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

---

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

10. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by their IT vendors to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Experian; (ix) statutory damages (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

12. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

### **PARTIES**

13. Plaintiff, Jilline Dobratz, is, and at all times mentioned herein was, an individual and citizen of West Bend, Wisconsin.

14. Defendant, The Medical College of Wisconsin, Inc., is a corporation incorporated under the state laws of Wisconsin with its principal place of business located in Milwaukee, Wisconsin.

15. Defendant, Progress Software Corporation, is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803.

### **JURISDICTION AND VENUE**

16. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Massachusetts and have different citizenship from PSC, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

17. This Court has jurisdiction over Defendants because Defendants operate in this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant PSC's principal place of business is located in this District, a substantial part of the

events giving rise to this action occurred in this District, and Defendants have harmed Class Members residing in this District.

## **FACTUAL ALLEGATIONS**

### ***Defendants' Businesses***

19. Defendant MCW is a corporation, based in Milwaukee, Wisconsin, that provides medical services to its patients.

20. Defendant PSC advertises itself as an “experienced, trusted provider of products designed with you, our customers, in mind. With Progress, you can build what you need, deploy where and how you want, empower your customers, then manage it all safely and securely.”<sup>6</sup>

21. Plaintiff and Class Members are current and former patients at MCW.

22. As a condition of obtaining medical services at MCW, Plaintiff and Class Members were required to entrust Defendants, directly or indirectly, with highly sensitive personal information.

23. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

24. Upon information and belief, MCW made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining medical services at MCW would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

---

<sup>6</sup> <https://www.progress.com/company>

25. Indeed, MCW's Privacy Policy provides that: "[t]his site has reasonable security measures in place to help protect against the loss, misuse, and alteration of the information under our control."<sup>7</sup>

26. Plaintiff and Class Members provided their Private Information, directly or indirectly, to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

27. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendants to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

28. Defendants had duties to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties, and MCW had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal duty to keep patients' Private Information safe and confidential.

29. Defendants had obligations created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

---

<sup>7</sup> <https://www.mcw.edu/about-mcw/terms-and-privacy>

30. Defendants derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendants could not perform the services they provide.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

### ***The Data Breach***

32. On or about November 14, 2023, MCW, on behalf of Defendants, began sending Plaintiff and other Data Breach victims a Notice of Security Incident letter (the "Notice Letter"), informing them that:

#### **What Happened?**

MCW received notice from one of our third-party vendors regarding a security vulnerability in the MOVEit Transfer solution which is utilized by MCW, MOVEit reported a vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on the MOVEit server. MOVEit has acknowledged the vulnerability and has since provided patches to remediate the exploit. There was no compromise of MCW's broader network security.

#### **What We Are Doing**

Upon being informed of the vulnerability, MCW immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third-party professionals to assist in the investigation and remediation of the vulnerability. Following our investigation, we discovered on September 21, 2023 that certain files containing your personal information were potentially removed from our MOVEit server by an unauthorized party on May 27, 2023. To date, Medical College of Wisconsin is now aware of any reports of identity theft or financial fraud for any information as a direct result of the incident.

#### **What Information Was Involved?**

The information potentially removed on the MOVEit server could have included your health insurance application and/or claim information, medical history, condition,

treatment, and/or diagnosis information, medical procedure information, patient dates of service, patient medical record number, and patient name.<sup>8</sup>

33. Omitted from the Notice Letter were the date that MCW was notified of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

34. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

35. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed. Moreover, MCW failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive Private Information.

36. The attacker accessed and acquired files from Defendants containing unencrypted Private Information of Plaintiff and Class Members, including their PHI and other sensitive information. Plaintiff’s and Class Members’ Private Information was accessed and stolen in the Data Breach.

---

<sup>8</sup> Notice Letter.

37. As Plaintiff has already experienced, the Private Information of Class Members was or will be subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

***Defendants Acquire, Collect, and Store Plaintiff's and Class Members' Private Information***

38. As a condition to obtain medical services at MCW, Plaintiff and Class Members were required to give their sensitive and confidential Private Information, directly or indirectly, to Defendants.

39. MCW retains and stores this information with PSC and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendants would be unable to perform their services.

40. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

41. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

42. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members or by MCW exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

43. Upon information and belief, Defendants made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

44. Indeed, MCW's Privacy Policy provides that: "[t]his site has reasonable security measures in place to help protect against the loss, misuse, and alteration of the information under our control."<sup>9</sup>

45. Defendants' negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

***Defendants Knew or Should Have Known of the Risk Because Healthcare Entities and Software Companies In Possession Of Private Information Are Particularly Susceptable To Cyber Attacks***

46. Data thieves regularly target companies like Defendants' due to the highly sensitive information that they custody. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

47. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities and software companies that collect and store Private Information, like Defendants, preceding the date of the breach.

48. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.<sup>10</sup>

---

<sup>9</sup> <https://www.mcw.edu/about-mcw/terms-and-privacy>

<sup>10</sup> See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

49. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

50. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>11</sup>

51. Additionally, as companies became more dependent on computer systems to run their business,<sup>12</sup> *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.<sup>13</sup>

---

<sup>11</sup>[https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=consumerprotection](https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection)

<sup>12</sup><https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

<sup>13</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

52. As custodians of Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if their data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

53. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

54. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

55. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' servers, amounting to more than two hundred thousand individuals' detailed Private Information,<sup>14</sup> and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

56. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

57. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—

---

<sup>14</sup> [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

particularly PHI—fraudulent use of that information and damage to victims may continue for years.

58. As a healthcare entity and software company in possession MCW’s patients’ Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if their data security systems, or those on which it transferred Private Information, were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

### ***Value Of Private Information***

59. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>15</sup> The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”<sup>16</sup>

60. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.<sup>17</sup>

---

<sup>15</sup> 17 C.F.R. § 248.201 (2013).

<sup>16</sup> *Id.*

<sup>17</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

61. For example, PII can be sold at a price ranging from \$40 to \$200.<sup>18</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>19</sup>

62. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>20</sup>

63. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.*, patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a “cyber black market” exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

64. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.<sup>21</sup> Indeed, during 2019 alone, over 41 million healthcare records were exposed,

---

<sup>18</sup> *Here’s How Much Your Private Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

<sup>19</sup> *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/>.

<sup>20</sup> *Medical I.D. Theft*, EFraudPrevention <https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.> (last visited Nov. 6, 2023).

<sup>21</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last accessed July 24, 2023).

stolen, or unlawfully disclosed in 505 data breaches.<sup>22</sup> In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.<sup>23</sup>

65. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.<sup>24</sup>

66. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief’s activities.”<sup>25</sup>

67. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.<sup>26</sup> Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.<sup>27</sup>

---

<sup>22</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed July 24, 2023).

<sup>23</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/> (last accessed July 24, 2023).

<sup>24</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021)

<sup>25</sup> Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last accessed July 24, 2023).

<sup>26</sup> See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July 24, 2023).

<sup>27</sup> *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/> (last accessed July 24, 2023).

68. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—names and PHI.

69. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”<sup>28</sup>

70. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

71. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>29</sup>

---

<sup>28</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

<sup>29</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

***Defendants Failed to Comply with FTC Guidelines***

72. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for patients’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

73. In October 2016, the FTC updated its publication, Protecting Private Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

74. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. These FTC enforcement actions include actions against healthcare entities and software companies, like Defendants.

77. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and MCW failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

78. Defendants were at all times fully aware of their obligations to protect the Private Information of MCW's patients yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

***MCW Failed to Comply with HIPAA Guidelines***

79. MCW is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

80. MCW is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).<sup>30</sup> See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

81. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

82. HIPAA’s Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

83. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

84. “Electronic protected health information” is “individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

85. HIPAA’s Security Rule requires MCW to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

---

<sup>30</sup> HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

86. HIPAA also requires MCW to “review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

87. HIPAA and HITECH also obligated MCW to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

88. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires MCW to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”<sup>31</sup>

89. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

---

<sup>31</sup> Breach Notification Rule, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

90. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

91. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.<sup>32</sup> The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.<sup>33</sup>

***Defendants Failed to Comply with Industry Standards***

92. As noted above, experts studying cybersecurity routinely identify healthcare entities and software companies as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

93. Some industry best practices that should be implemented by healthcare entities and software companies dealing with sensitive Private Information, like Defendants, include but

---

<sup>32</sup> <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

<sup>33</sup> <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

94. Other best cybersecurity practices that are standard in the health care and software industries include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

95. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

96. Defendants failed to comply with these accepted standards in the healthcare and software industries, thereby permitting the Data Breach to occur.

***Defendants Breached Their Duties to Safeguard Plaintiff's and the Class's Private Information***

97. In addition to their obligations under federal and state laws, Defendants owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed

duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Class Members

98. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data, and MCW failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect MCW's patients' Private Information;
- c. Failing to properly monitor their own data security systems for existing intrusions;
- d. Failing to sufficiently train their employees and vendors regarding the proper handling of MCW's patients' Private Information;
- e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- f. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,
- g. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

99. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access their computer networks and systems which contained unsecured and unencrypted Private Information.

100. Had Defendants remedied the deficiencies in their information storage and security systems or those of their vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

***Common Injuries & Damages***

101. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

***The Data Breach Increases Victims' Risk Of Identity Theft***

102. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

103. As Plaintiff has already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

104. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

105. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

106. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

107. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.<sup>34</sup>

108. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

109. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

---

<sup>34</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than MCW credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

110. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like Social Security numbers) of Plaintiff and the other Class Members.

111. Thus, even if certain information (such as Social Security numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

112. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

***Loss Of Time To Mitigate Risk Of Identity Theft And Fraud***

113. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

114. Thus, due to the actual and imminent risk of identity theft, MCW, in its Notice Letter, instructs Plaintiff and Class Members to take the following measures to protect themselves:

Enclosed in this notice letter are steps that we encourage you to take to protect yourself against misuse of your personal information. In addition to the steps provided below, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.<sup>35</sup>

115. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result

---

<sup>35</sup> Notice Letter.

of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring their own computer networks, and contacting credit bureaus to place fraud alerts on their accounts.

116. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>36</sup>

117. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>37</sup>

118. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>38</sup>

---

<sup>36</sup> See United States Government Accountability Office, GAO-07-737, Private Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

<sup>37</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

<sup>38</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

***Diminution Value Of Private Information***

119. PII and PHI are valuable property rights.<sup>39</sup> Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

120. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>40</sup>

121. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>41,42</sup>

122. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>43</sup>

123. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.<sup>44</sup>

124. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,

---

<sup>39</sup> See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

<sup>40</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>41</sup> <https://datacoup.com/>

<sup>42</sup> <https://digi.me/what-is-digime/>

<sup>43</sup> Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

<sup>44</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>45</sup>

125. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.<sup>46</sup>

126. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

127. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change, e.g., names and PHI.

128. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

129. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

<sup>45</sup> *Medical I.D. Theft, EFraudPrevention*  
<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected>. (last visited Nov. 6, 2023).

<sup>46</sup> Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021)

130. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

131. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to more than two hundred thousand individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

132. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

***Future Cost of Credit & Identity Theft Monitoring is Reasonable and Necessary***

133. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, the volume of data obtained in the Data Breach, and Plaintiff's Private Information already being disseminated on the dark web (as discussed below), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

134. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to

file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

135. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

136. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

***Loss Of The Benefit Of The Bargain***

137. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain medical services at MCW under certain terms, Plaintiff and other reasonable patients understood and expected that they were, in part, paying for the necessary data security to protect the Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received medical services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with MCW.

***Plaintiff Dobratz's Experience***

138. Plaintiff Jilline Dobratz is a former MCW patient who obtained services there in or about 2017.

139. As a condition of obtaining medical services at MCW, Plaintiff was required to provide her Private Information, directly or indirectly, to Defendants, including her name, PHI, and other sensitive information.

140. At the time of the Data Breach—on or about May 27, 2023—Defendants retained Plaintiff's Private Information in their systems, despite Plaintiff no longer being a MCW patient for approximately six years.

141. Plaintiff Dobratz is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendants had she known of Defendants' lax data security policies.

142. Plaintiff Dobratz received the Notice Letter, by U.S. mail, from MCW, dated November 14, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, health insurance application and/or claim information, medical history, condition, treatment, and/or diagnosis information, medical procedure information, patient dates of service, and patient medical record number.

143. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring her own computer network, and contacting credit bureaus to place fraud alerts on her accounts. Plaintiff has spent significant time on reasonable efforts to mitigate the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

144. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

145. Plaintiff also suffered actual injury in the form of her Private Information being disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

146. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

147. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

149. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

150. Plaintiff Dobratz has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

### **CLASS ACTION ALLEGATIONS**

151. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

152. Specifically, Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

#### **Nationwide Class**

All individuals in the United States whose Private Information was impacted as a result of the Data Breach (the "Class").

#### **Wisconsin Subclass**

All individuals in the state of Wisconsin whose Private Information was impacted as a result of the Data Breach (the "Wisconsin Subclass").

153. Excluded from the Classes are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

154. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class and/or Wisconsin Subclass as well as add subclasses, before the Court determines whether certification is appropriate.

155. The proposed Classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

156. Numerosity: The Class Members are so numerous that joinder of all members is impracticable. Although the exact number of Class Members is currently unknown to Plaintiff and exclusively in the possession of Defendants, according to the breach report submitted to the U.S. Department of Health and Human Services, at least 240,000 persons were impacted in the Data Breach.<sup>47</sup> The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by MCW sending them Notice Letters).

157. Commonality: There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants engaged in the conduct alleged herein;
- b. Whether Defendants' conduct violated the FTCA;
- c. When Defendants learned of the Data Breach;
- d. Whether Defendants' response to the Data Breach was adequate;
- e. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;
- f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

---

<sup>47</sup> [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

- i. Whether Defendants owed duties to Class Members to safeguard their Private Information;
- j. Whether Defendants breached their duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Breach;
- l. Whether Defendants had legal duties to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether Defendants breached their duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;
- p. Whether Defendants' conduct was negligent;
- q. Whether Defendants were unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

158. Typicality: Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiff are advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

159. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

160. Predominance: Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

161. Superiority: A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

162. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

163. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice Letters by MCW.

**COUNT I**  
**Negligence**  
**(On Behalf of Plaintiff and the Class against Defendants)**

164. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein, and brings this claim against both Defendants.

165. MCW requires its patients, including Plaintiff and Class Members, to submit non-public Private Information to Defendants in the ordinary course of providing its services.

166. MCW gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

167. Plaintiff and Class Members entrusted Defendants, directly or indirectly, with their Private Information with the understanding that Defendants would safeguard their information.

168. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

169. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants owed duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. MCW's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

170. Defendants had duties to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

171. MCW's duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

172. For instance, HIPAA required MCW to notify victims of the Breach within 60 days of the discovery of the Data Breach. MCW did not begin to notify Plaintiff or Class Members of the Data Breach until November 14, 2023 despite, upon information and belief, MCW knowing

shortly after May 27, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiff and the Class.

173. Defendants owed duties of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

174. Defendants' duties of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential Private Information, a necessary part of being patients at MCW.

175. Defendants' duties to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

176. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

177. Defendants also had duties to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

178. Moreover, Defendants had duties to promptly and adequately notify Plaintiff and the Class of the Data Breach.

179. Defendants had and continues to have duties to adequately disclose that the Private Information of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised

and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

180. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

181. Defendants violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

182. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

183. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

184. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

185. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

186. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare and software industries.

187. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

188. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

189. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

190. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

191. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

192. Defendants' duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

193. MCW has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

194. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

195. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

196. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Experian; (ix) statutory damages (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

197. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

198. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

199. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

200. Defendants' negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

201. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT II**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiff and the Class against Defendant MCW)**

202. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this count solely against Defendant MCW ("Defendant" for the purposes of this count).

203. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of receiving medical services from Defendant.

204. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

205. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

206. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

207. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

208. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

209. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

210. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class

Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

211. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

212. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

213. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

214. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

215. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

216. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

217. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

218. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

219. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT III**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Class against Defendants)**

220. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein, and brings this claim against both Defendants.

221. This Count is pleaded in the alternative to the breach of contract count above.

222. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for or had payments made on their behalf for medical services from MCW as well as provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have received from MCW the medical services from MCW that were the subject of the transaction and should have had their Private Information protected with adequate data security.

223. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

224. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

225. Defendants acquired the Private Information through inequitable record retention as they failed to disclose the inadequate data security practices previously alleged.

226. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendants or obtained medical services at MCW.

227. Plaintiff and Class Members have no adequate remedy at law.

228. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

229. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Experian; (ix) statutory damages (x) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as

Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

230. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

231. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**COUNT IV**  
**Violation of The Right To Privacy Act,**  
**Wis. Stat. § 995.50(2)**  
**(On Behalf of Plaintiff and the Wisconsin Subclass against Defendant MCW)**

232. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this count solely against Defendant MCW (“Defendant” for the purposes of this count) on behalf of herself and the Wisconsin Subclass (the “Class” for the purposes of this count).

233. Wisconsin has codified the traditional common law torts of invasion of privacy and intrusion upon seclusion through Wis. Stat. § 995.50(2).

234. Defendant violated the Wisconsin Right to Privacy statute by publicizing private details and facts in a place that a reasonable person would consider private, not generally known to the public, not publicly available, without consent and not of legitimate public concern about Plaintiff and Class Members by disclosing and exposing Plaintiff’s and Class Members’ PII and

PHI to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

235. The disclosure of Plaintiff's and Class Members' PII and PHI is harmful and highly offensive to a reasonable person of ordinary sensibilities.

236. Defendant should appreciate that the cyber-criminals who stole the PII and PHI would further sell and disclose the PII and PHI and that the original disclosure is devastating to the Plaintiff and the Class Members even though it may have originally only been made to one person or a limited number of cyber-criminals.

237. Under Wisconsin's Right to Privacy statute, the tort of public disclosure of private facts is recognized in Wisconsin. Plaintiff's and the Class Members' private PII and PHI was publicly disclosed by Defendant in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew and knows that Plaintiff's and Class Members' PII and PHI is not a matter of legitimate public concern.

238. The Wisconsin Right to Privacy statute provides that any person whose privacy is unreasonably invaded is entitled to the following relief: (a) Equitable relief to prevent and restrain such invasion, excluding prior restraint against constitutionally protected communication privately and through the public media; (b) Compensatory damages based either on plaintiff's loss or defendant's unjust enrichment; and (c) A reasonable amount for attorney fees." Wis. Stat. § 995.50(2)(1)(a)-(c).

239. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members privacy have been unreasonably invaded and are entitled to equitable relief to prevent and restrain ongoing or future invasions of privacy, compensatory damages based on the harm

Plaintiff and Class Members suffered, or alternatively compensatory damages based on Defendant's being unjustly enriched by its conduct.

**COUNT V**

**Violation of Wisconsin Confidentiality Of Health Records Law,  
Wis. Stat. §146.81, *et seq.*  
(On Behalf of Plaintiff and the Wisconsin Subclass against Defendant MCW)**

240. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this count solely against Defendant MCW ("Defendant" for the purposes of this count) on behalf of herself and the Wisconsin Subclass (the "Class" for the purposes of this count).

241. Wisconsin law regarding Confidentiality of Patient Health Care Records states that:

All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient."

Wis. Stat. §146.82(1).

242. Defendant disclosed the private and protected medical information of Plaintiff and Class members to unauthorized third parties without their knowledge, consent, or authorization.

243. Plaintiff and Class Members provided their Private Information to MCW, which is a "health care provider" as defined by Wis. Stat. § 146.81(1).

244. Plaintiff and Class Members are "patients," as defined by Wis. Stat. § 146.81(3).

245. The stolen Private Information belonging to Plaintiff and Class Members are "health care records" under Wis. Stat. § 146.81(4).

246. Defendant is a "covered entity" for purposes of Wis. Stat. § 146.82 and had a duty not to disclose any healthcare records in its possession regarding Plaintiff and members of the Class. Wis. Stat. § 146.82.

247. Defendant disclosed healthcare care records pertaining to Plaintiff and Class Members without their consent and for no other reason permitted by either Wis. Stat. § 146.82(5) or § 610.70, and therefore violated Wis. Stat. § 146.82.

248. Defendant violated Wis. Stat. §§146.81, *et seq.* through its willful and knowing failure to maintain adequate security measures, which allowed criminals to improperly access and compromise when it compromised, allowed access to, released, and disclosed patient health care records and Private Information without the informed consent or authorization of Plaintiff and Class Members. Defendant did not and does not have express or implied consent to disclose, allow access to, or release the Plaintiff's and Members' Private Information. To the contrary, Defendant expressly undertook a duty and obligation to Plaintiff and Class Members.

249. Plaintiff and Class Members were injured and have suffered damages as a result of Defendants illegal disclosure and negligent release of their healthcare records in violation of Wis. Stat. § 146.82.

250. Defendant did not disclose to or warn the Plaintiff and Class Members that their Private Information could be compromised, stolen, released, or disclosed to third parties without their consent as a result of Defendant's computer systems (or those of its vendors) and software being outdated, easy to hack, inadequate, and insecure. Plaintiff and Class Members did not know or expect, or have any reason to know or suspect, that Defendant's computer systems (or those of its vendors) and software were so outdated, easy to hack, inadequate, and insecure that it would expose their Private Information to unauthorized disclosure.

251. Wis. Stat. §146.84(1)(b) states:

Any person, including the state or any political subdivision of the state, who violates Wis. Stat. § 146.82 or § 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than \$25,000 and costs and reasonable attorneys' fees.

252. Wis. Stat. §146.84(1)(bm) states:

Any person, including the state or any political subdivision of the state, who negligently violates Wis. Stat. §146.82 or 146.83 shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than \$1,000 and costs and reasonable actual attorney fees. Wis. Stat. §146.84(1)(bm).

253. Wis. Stat. §146.84(1)(c) states:

An individual may bring an action to enjoin any violation of §§146.82 or 146.83 or to compel compliance with §§146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection.

254. Actual damages are not a prerequisite to liability for statutory or exemplary damages under Wis. Stat. §146.81. A simple comparison of other Wisconsin statutes (*e.g.*, Wis. Stat. §134.97(3)(a) and (b), “Civil Liability; Disposal And Use” of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. §146.84 when it explicitly did so in other privacy statutes. *See* Wis. Stat. §134.97(3)(a) and (b).

255. Similarly, the Wisconsin legislature made it clear that the exemplary damages referred to Wis. Stat. §146.81 are not the same as punitive damages. Here, the plain language of another Wisconsin statute (Wis. Stat. §895.043(2), “Scope” of punitive damages), specifically and unequivocally excludes an award of “exemplary damages” under Wis. Stat. §§146.84(1)(b) and (bm) from the scope of “punitive damages” available under Section 895.043. In short, exemplary damages under Wis. Stat. §146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been “injured” as a result of a negligent data breach like the one at issue here.

256. Plaintiff and Class Members request that the Court issue declaratory relief declaring Defendant’s practice of using insecure, outdated, and inadequate email and computer

systems and software that are easy to hack for storage and communication of Private Information data between Defendant and third parties. The Plaintiff and Class Members further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and enjoining Defendant from disclosing or using Private Information without first adequately securing or encrypting it.

257. Plaintiff and Class Members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing Private Information in their possession or the possession of third parties and provide it to the Plaintiff and Class Members.

258. Plaintiff and Class Members request that the Court enter an injunction ordering that Defendant:

- a. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit Defendant's safeguards and procedures on a periodic basis;
- b. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;
- c. conduct regular checks and tests on its safeguards and procedures;
- d. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;
- e. meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendant is taking to update its security technology to adequately secure and safeguard patient Private Information; and

- f. identify to each Class Member in writing with reasonable specificity the Private Information of each such Class Member that was stolen in the Data Breach, including without limitation as required under Wis. Stat. §134.98(3)(c).

259. Additionally, Plaintiff and Class Members request the Court enter an Order pursuant to Wis. Stat. §146.84(1)(bm) awarding minimum statutory exemplary damages of \$1,000 to Plaintiff and each Class Member whose Private Information was compromised and stolen, as well as attorneys' fees and costs.

**COUNT VI**  
**Violation of the Wisconsin Deceptive Trade Practices Act,**  
**Wis. Stat. §§100.18, *et seq.*,**  
**(On Behalf of Plaintiff and the Wisconsin Subclass against Defendant MCW)**

260. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein and brings this count solely against Defendant MCW ("Defendant" for the purposes of this count) on behalf of herself and the Wisconsin Subclass (the "Class" for the purposes of this count).

261. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act (the "WDTPA"), which provides that no,

"firm, corporation or association,. . .with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

Wis. Stat. § 110.18.

262. Defendant is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

263. Plaintiff and Class Members are members of “the public,” as defined by Wis. Stat. § 100.18(1).

264. Plaintiff and Class Members “suffered pecuniary loss because of a violation” of the WDTPA. Wis. Stat. §100.18(11)(b)(2).

265. Defendant deliberately engaged in deceptive and unlawful practices and violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services (and those of its vendors) by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; (b) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; (c) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems (or those of its vendors) and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; and (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact reasonable security practices to safeguard its systems (or those of its vendors) and data from cyberattacks like the Data Breaches.

266. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions, and therefore increase the sales of Defendant’s medical services.

267. Defendant’s representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Class members, about the adequacy of

Defendant's security measures (or those of its vendors) and ability to protect the confidentiality of consumers' Private Information.

268. Defendant's representations and omissions were further material because they were likely to deceive reasonable consumers, including Plaintiff and Class members, that their Private Information was not exposed and misled Plaintiff and Class Members into believing they did not need to take actions to secure their Private Information exposed by Defendant.

269. Defendant knew or should have known that its computer systems and security practices and procedures (and those of its vendors) were inadequate, and that risk of the Data Breaches and theft was high. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

270. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from time and expense relating to monitoring their Private Information for fraudulent activity, an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

271. Defendant had an ongoing duty to Plaintiff and Class members to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18. 405.

272. Plaintiff and the Class Members reasonably relied upon Defendant's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendants and that the Court grants the following:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Wisconsin Subclass, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the

retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
- v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;
- ix. requiring Defendants to conduct regular database scanning and securing checks;

- x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;
- xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their

confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect herself;

- xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and
- xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;
- E. For an award of punitive damages, as allowable by law;
- F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as this court may deem just and proper.

#### **DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all triable issues.

DATED: December 5, 2023

Respectfully submitted,

/s/ Randi Kassan

Randi Kassan (MA Bar No. 568565)

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN, LLC**

100 Garden City Plaza

Garden City, NY 11530

Telephone: (212) 594-5300

rkassan@milberg.com

*Counsel for Plaintiff and the Proposed Class*